RM-11699: Encryption of Amateur Radio Communications
Name of Filer: Dr. Donald Bindner

Comments: Let me recommend AGAINST the adoption and expansion of encryption for amateur radio communications.

I understand the desire to allow encrypted communication on amateur frequencies for use during emergencies. In particular, medical institutions feel they are squeezed between the privacy requirements of HIPAA and the openness of amateur communications when hams support them during emergencies. This is not a compelling enough reason to expand the use of encrypted communication onto amateur frequencies.

The two strongest reasons not to expand the use of encryption for hams are 1) it will not work for the scenario for which it is desired, emergencies; and 2) it will undermine and corrupt the honest use of amateur frequencies.

1.) *Encryption will not be effective in emergencies.* We learned this from the Global Positioning System during the Gulf War. Previous to the Gulf War, GPS signals were encrypted so that civilian receivers had "less than military precision." During the war, it was the case that the military was using civilian receivers widely through the ranks, and the encryption was temporarily disabled. It has since been permanently disabled.

It was precisely during an engagement where encryption should have been desirable that it was found to be a hindrance. It is even more likely that encryption will hinder more than help in a situation that employs a diverse group of amateur volunteers. It is almost certain. Even with practice, emergencies are chaotic changing events.

This has happened with police departments with the change to narrow-band and digital communications. Our local department programmed their radios for *digital* narrow band on the "mutual aid" frequency, while the Missouri State Patrol programmed their radios for *analog* narrow band. The result was that the two could not communicate during a man-hunt, and our local officers were told to "go home" because they were hindering the search. Emergencies are times where everything has to work and everything has to be compatible, and encryption is the opposite of that.

2.) *Encryption undermines and corrupts the appropriate use of amateur frequencies.* I am young enough and technical enough to use encryption over the air if I desire. I have implemented encryption technologies in software and discovered encryption bugs in other projects. I have several times desired to be able to use encryption and ham radio together, but every time I have had that temptation it was because I was wanting to do something that was essentially *inappropriate for amateur radio.*

Amateur radio is a self-policing endeavor. Not only do hams listen and report

activities that are inappropriate, they also show personal individual restraint. They follow the rules. Everyone knows "someone" may be listening, and this has the effect of preemptive encouraging people to explore radio within the intent of the law.

The encouragement of encryption undermines this self-restraint. It also damages the ability of hams to "listen in" and learn from exchanges that they are not necessarily part of. It simultaneously makes the legitimate activity of amateur radio less effective and encourages hams to be less honorable.

Conclusion: The appropriate legislative change to make with regard to sensitive communications is to relax privacy requirements during emergencies. Already the law allows amateurs to break rules when there are serious threats to life and property. Privacy requirements for hospitals should be relaxed for medical institutions and personnel under similar circumstances.

The suspension of HIPAA in emergencies is not likely to be abused. Medical institutions and personnel have a culture of privacy preservation and ethical attention to the well-being of their patients.

Suspending the requirements will be more useful in emergencies than encrypted communications, and it will not corrupt the practice of amateur radio.

Donald J. Bindner — `kd0pgm`
22463 State Highway H
Kirksville, MO 63501